McDATA™

Networking the world's business data™

McDATA PRODUCTS

McDATA 4416
Fibre Channel Switch Module
Installation Guide

P/N 59180-00
REV A

Simplifying Storage Network Management

McDATA Corporation
380 Interlocken Crescent Broomfield, CO 80021-3464
Corporate Headquarters: 800-545-5773
Sales E-mail: sales@mcdata.com *Web:* www.mcdata.com

Record of Revisions and Updates

Revision	Date	Description
59180-00 A	01/13/06	Release

Printed January 2006

First Edition

Contents

Notes

Figures

Notes

Tables

Notes

Preface

This manual describes the features and installation of the McDATA 4416 switch module, firmware version 5.2.3.

Who Should Use this Manual

This manual introduces users to the switch module and explains its installation and service. It is intended for users who are responsible for installing and servicing network equipment.

How to Use this Manual

This publication is organized as follows:

- Chapter 1 is an overview of the switch module. It describes the ports and indicator LEDs.
- Chapter 2 describes the factors to consider when planning a fabric.
- Chapter 3 explains how to install and configure the switch.
- Chapter 4 describes the diagnostic methods and troubleshooting procedures.
- Appendix A lists the switch module specifications.

A glossary and an index are also provided.

Related Documentation

Other publications that provide additional information about the McDATA 4416 switch module are:

- *McDATA 4416 Product Information Guide*, publication number, 59179-00.
- *McDATA 4416 Quick Start Guide*, publication number 50562-00.
- *McDATA Switch Module Management Guide*, publication number 59181-00.
- *McDATA 4416 Command Line Interface Guide*, publication number 59182-00.
- Fibre Channel-Arbitrated Loop (FC-AL-2) Rev. 6.8.
- Fibre Channel-10-bit Interface Rev. 2.3.
- Definitions of Managed Objects for the Fabric Element in Fibre Channel Standard (draft-ietf-ipfc-fabric-element-mib-04.txt).

The Fibre Channel Standards are available from:

Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112-5776 Phone: (800) 854-7179 or (303) 397-7956
Fax: (303) 397-2740.

1 General Description

This section describes the features and capabilities of the McDATA 4416 Fibre Channel Switch Module in a server blade chassis. The following topics are described:

- Switch Module Controls and LEDs
- Fibre Channel Ports
- Ethernet Port
- Switch Module Management

Fabrics are managed with the McDATA Embedded Web Server™ switch management application (version 5.02.03) and the Command Line Interface (CLI). With the Element Manager Product Features Enabled (PFE) key, you can manage a single switch through EFCM using McDATA Element Manager™. Refer to the *McDATA Switch Module Management Guide* for information about using the McDATA Embedded Web Server application and McDATA Element Manager. Refer to the *McDATA 4416 Command Line Interface Guide* for more information about the command line interface.

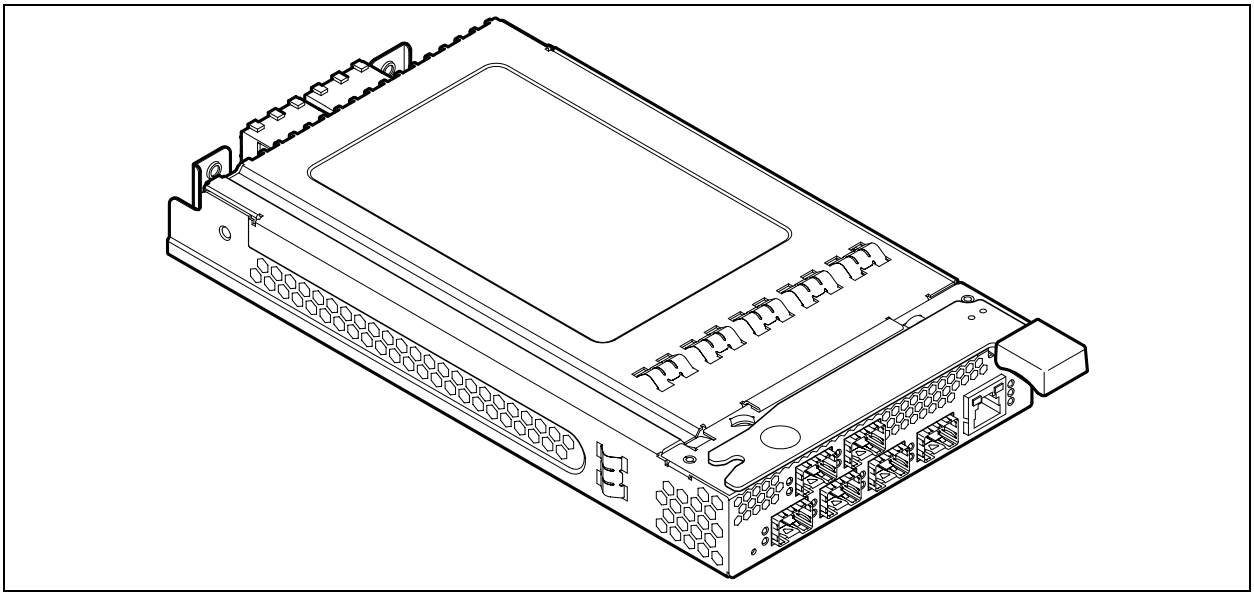

Figure 1-1. McDATA 4416 Switch Module

Switch Module Controls and LEDs

The switch module LEDs provide information about the switch module's operational status. These LEDS include the Identifier LED, System Fault LED, and Input Power LED. The Maintenance button shown in Figure 1-2 is the only switch module control and is used to reset a switch module or to recover a disabled switch module.

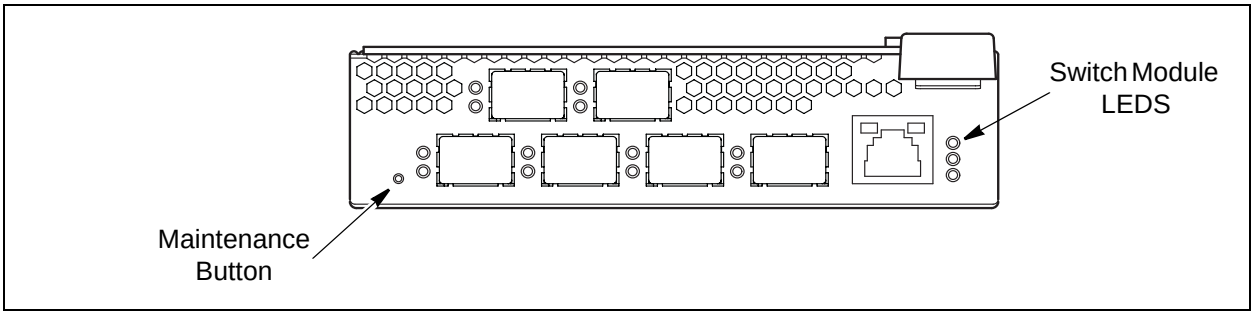

Figure 1-2. Switch Module Controls and LEDS

Maintenance Button

The Maintenance button is a dual-function momentary switch on the front panel. Its purpose is to reset the switch module or to place the switch module in maintenance mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch module for maintenance purposes when flash memory or the resident configuration file is corrupted. Refer to "Recovering a Switch Module" on page 4-5 for more information about using maintenance mode.

Resetting a Switch

To reset the switch module, use a pointed tool to momentarily press and release (less than 2 seconds) the Maintenance button. The switch module will respond as follows:

1. All switch module LEDs will illuminate, then the System Fault LED extinguishes leaving only the Input Power LED illuminated.
2. After approximately 1 minute, the power-on self test (POST) begins.
3. When the POST is complete, the Input Power LED is illuminated.

Placing the Switch in Maintenance Mode

To place the switch module in maintenance mode, do the following:

1. Isolate the switch module from the fabric.
2. Press and hold the Maintenance button with a pointed tool for 2–4 seconds.
3. After a few seconds, the POST begins illuminating all switch module LEDs.
4. When the POST is complete, the switch module LEDs extinguish.

To exit maintenance mode and return to normal operation, momentarily press and release the Maintenance button to reset the switch module.

Switch Module LEDs

The switch module LEDs shown in Figure 1-3 provide status information about switch module operation. Refer to "External Port LEDs" on page 1-5 for information about port LEDs.

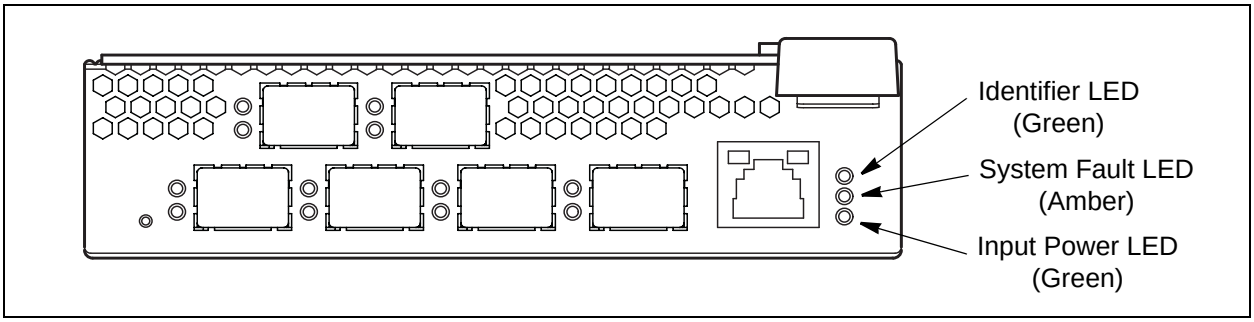

Figure 1-3. Switch Module LEDs

Identifier LED (Green)

The Identifier LED identifies a specific switch module through the server blade interface.

Input Power LED (Green)

The Input Power LED indicates the voltage status at the switch module logic circuitry. During normal operation, this LED illuminates to indicate that the switch module logic circuitry is receiving the proper DC voltages. When the switch module is in maintenance mode, this LED is extinguished.

System Fault LED (Amber)

The System Fault LED illuminates to indicate an over temperature condition or a Power on Self Test (POST) error.

Fibre Channel Ports

The switch module has 6 external Fibre Channel ports through which to connect to devices or other switches and 10 internal ports connecting to the server midplane. Each of the external Fibre Channel ports is served by a Small Form-Factor Pluggable (SFP) optical transceiver and is capable of 1-Gbps, 2-Gbps, or 4-Gbps transmission. SFPs are hot-pluggable. External ports can self-discover both the port type and transmission speed when connected to public devices or other switches. The internal ports operate at 1-Gbps or 2-Gbps.

The external ports are named Ext10, Ext11, Ext12, Ext13, Ext14, and Ext15 and are numbered 10–15 as shown in Figure 1-4. The external port LEDs are located to the left their respective ports and provide port login and activity status information.

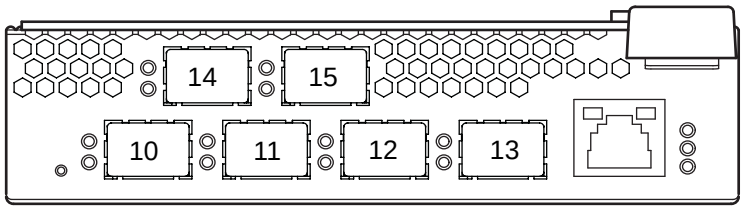

Figure 1-4. Fibre Channel Ports

Internal ports are named Int0–Int9 and numbered 0–9. The port numbers 0–9 correspond to server blades 1–10 as shown in Figure 1-5.

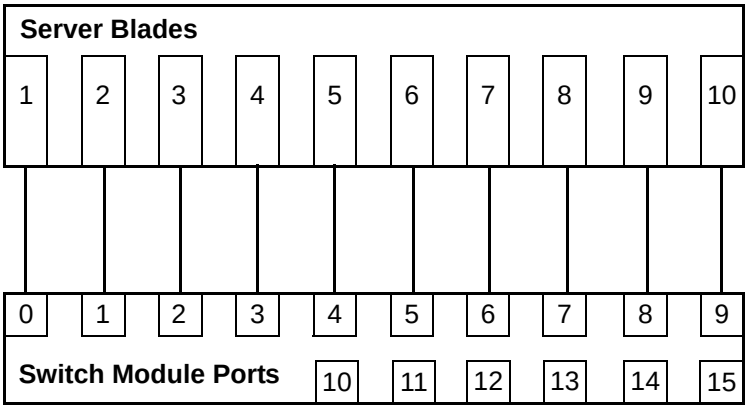

Figure 1-5. Internal Port/Server Blade Mapping

NOTE: The switch module comes from the factory as a 12-port switch, enabling external ports 10–13 and internal ports 0–7 . You can upgrade the switch module to enable the remaining external ports (14, 15) and internal ports (8, 9) through the purchase of the Port Activation PFE key. Refer to the *McDATA Switch Module Management Guide* for information about installing a PFE key. For additional McDATA PFE keys, please contact your McDATA representative or visit the web site at www.mcdata.com.

External Port LEDs

Each external port has its own Logged-In LED (L) and Activity LED (A) as shown in Figure 1-6.

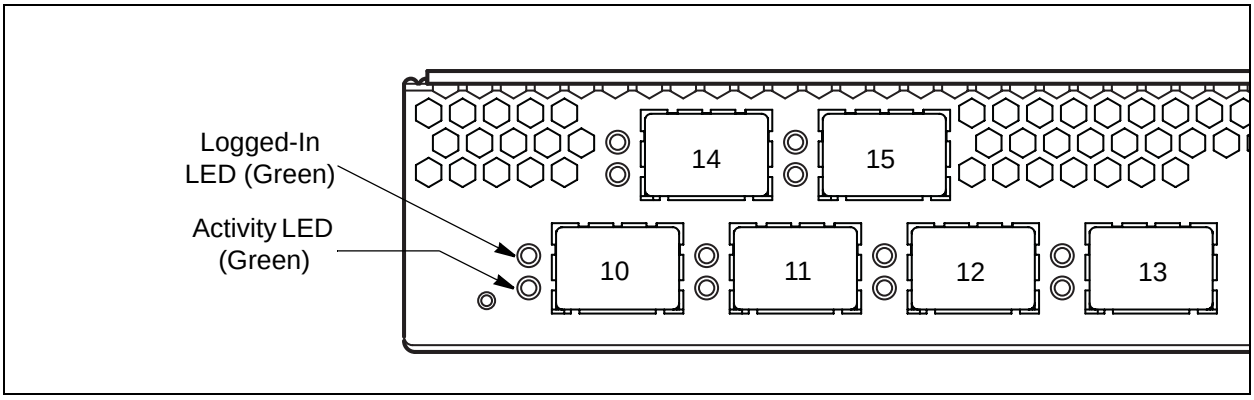

Figure 1-6. External Port LEDs

Port Logged-In LED (Green)

The Logged-in LED indicates the logged-in or initialization status of the connected devices. After successful completion of the POST, the switch module extinguishes all Logged-In LEDs. Following a successful loop initialization or port login, the switch module illuminates the corresponding logged-in LED. This shows that the port is properly connected and able to communicate with its attached devices. The Logged-In LED remains illuminated as long as the port is initialized or logged in. If the port connection is broken or an error occurs that disables the port, the Logged-In LED will flash. Refer to "Logged-In LED Indications" on page 4-2 for more information about the Logged-In LED.

Port Activity LED (Green)

The Activity LED indicates that data is passing through the port. Each frame that the port transmits or receives causes this LED to illuminate for 50 milliseconds. This makes it possible to observe the transmission of a single frame. When extending credits, the Activity LED for a donor port will reflect the traffic of the recipient port. Refer to "Distance" on page 2-4 for more information about extended credits and donor ports.

Transceivers

Switch modules support SFP optical transceivers for the Fibre Channel ports. A transceiver converts electrical signals to and from optical laser signals to transmit and receive data. Duplex fiber optic cables plug into the transceivers which then connect to the devices. A Fibre Channel port is capable of transmitting at 1-Gbps, 2-Gbps, or 4-Gbps; however, the transceiver must also be capable of delivering at these rates.

The SFP transceivers are hot pluggable. This means that you can remove or install a transceiver while the switch module is operating without harming the switch module or the transceiver. However, communication with the connected device will be interrupted. Refer to "Install SFP Transceivers" on page 3-2 for information about installing and removing SFP optical transceivers.

Port Types

Switch modules support generic ports (G_Port, GL_Port), fabric ports (F_Port, FL_Port), and expansion ports (E_Port). Switch modules come from the factory with internal ports configured as FL_Ports and external ports configured as GL_Ports. Generic, fabric, and expansion ports function as follows:

- A GL_Port self-configures as an FL_Port when connected to a public loop device, as an F_Port when connected to a single public device, or as an E_Port when connected to another switch. If the device is a single device on a loop, the GL_Port will attempt to configure first as an F_Port, then if that fails, as an FL_Port.
- A G_Port self-configures as an F_Port when connected to a single public device, or as an E_Port when connected to another switch.
- An FL_Port supports a loop of up to 126 public devices. An FL_Port can also configure itself during the fabric login process as an F_Port when connected to a single public device (N_Port).
- An F_Port supports a single public device.

E_Ports enable you to expand the fabric by connecting switch modules with other switches. Switch modules self-discover all inter-switch connections. Refer to "Multiple Chassis Fabrics" on page 2-6 for more information about multiple chassis fabrics. Refer to the *McDATA Switch Module Management Guide* for information about defining port types.

Ethernet Port

The Ethernet port shown in Figure 1-7 is an RJ-45 connector that provides a connection to a management workstation through a 10/100 Base-T Ethernet cable. A management workstation can be a Windows® or a Linux® workstation that is used to configure and manage the switch fabric. The switch through which the fabric is managed is called the fabric management switch. You can manage the switch module over an Ethernet connection with the following management tools:

- McDATA Embedded Web Server
- McDATA Element Manager through EFCM
- Command Line Interface (CLI)
- Simple Network Management Protocol (SNMP)

The Ethernet port has two LEDs: the Link Status LED (green) and the Activity LED (green). The Link Status LED illuminates continuously when an Ethernet connection has been established. The Activity LED illuminates when data is being transmitted or received over the Ethernet connection.

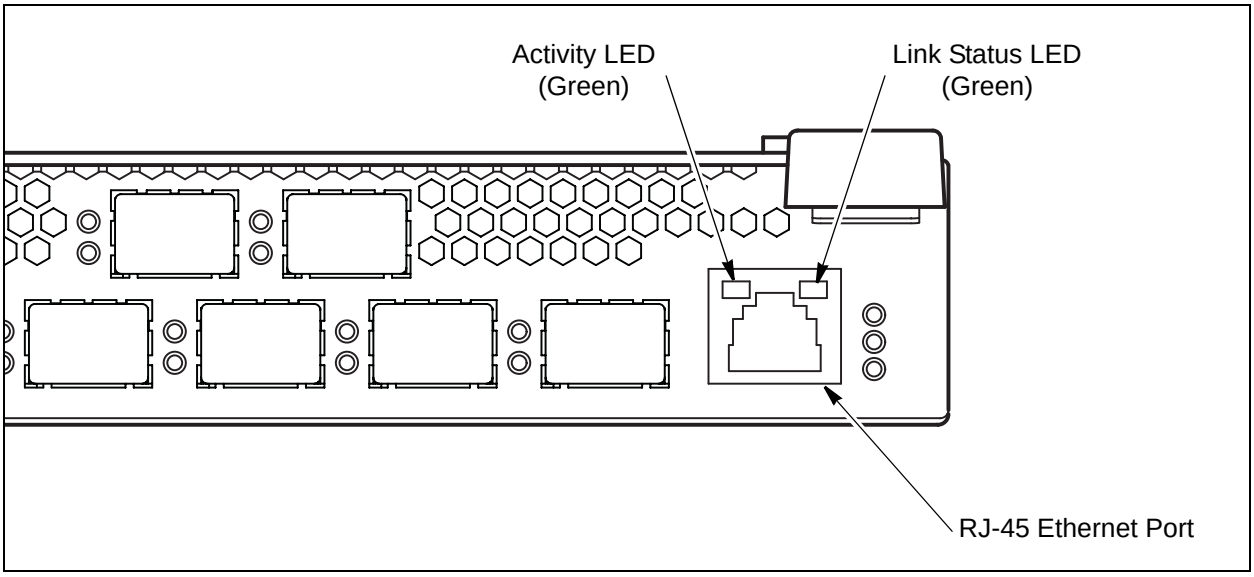

Figure 1-7. Ethernet Port

Switch Module Management

The switch supports the following management tools:

- McDATA Embedded Web Server
- McDATA Element Manager
- Command Line Interface
- Simple Network Management Protocol
- File Transfer Protocol

McDATA Embedded Web Server

McDATA Embedded Web Server is a graphical user interface that provides both fabric and switch module management functions. Because McDATA Embedded Web Server resides in the switch firmware, no installation is needed. You can run one instance of the McDATA Embedded Web Server at a time by opening the switch IP address with an internet browser. Refer to the *McDATA Switch Module Management Guide* for information about the McDATA Embedded Web Server.

McDATA Element Manager

McDATA Element Manager is a subset of the McDATA Embedded Web Server and enables you to manage a single switch through EFCM. To open McDATA Element Manager through EFCM, you must install the Element Manager (PFE) key on the switch module. For information about McDATA Element Manager and its capabilities, refer to the *McDATA Switch Module Management Guide*.

Command Line Interface

The command line interface (CLI) provides monitoring and configuration functions by which the administrator can manage the fabric and its switches. The CLI is accessible over an Ethernet connection. Refer to *McDATA 4416 Command Line Interface Guide* for more information.

Simple Network Management Protocol

SNMP provides monitoring and trap functions for the fabric. The switch module firmware supports SNMP versions 1 and 2, the Fibre Alliance Management Information Base (FA-MIB) version 4.0, and the Fabric Element Management Information Base (FE-MIB) RFC 2837. Traps can be formatted using SNMP version 1 or 2.

File Transfer Protocol

FTP provides the command line interface for exchanging files between the switch module and the management workstation. These files include firmware image files, configuration files, and log files. Refer to the *McDATA 4416 Command Line Interface Guide* for an example of using FTP to transfer configuration backup files.

2 Planning

Consider the following when planning a fabric:

- Devices
- Device Access
- Performance
- Multiple Chassis Fabrics
- Switch Module Services
- Fabric Security
- Fabric Management

Devices

When planning a fabric, consider the number of public devices and the anticipated demand. This will determine the number of ports that are needed and in turn the number of switches.

The switch module uses SFP optical transceivers, but the device host bus adapters you are using may not. Consider whether the device adapters use SFP or Gigabit Interface Converters (GBIC) transceivers, and choose fiber optic cables accordingly. Use LC-type cable connectors for SFP transceivers and SC-type cable connectors for GBIC transceivers. Also consider the transmission speed compatibility of your devices, HBAs, switches, and SFPs.

Consider the distribution of targets and initiators. An F_Port supports a single public device. An FL_Port can support up to 126 public devices in an arbitrated loop.

Device Access

Consider device access needs within the fabric. Access is controlled by the use of zones and zone sets. Some zoning strategies include the following:

- Group devices by operating system.
- Separate devices that have no need to communicate with other devices in the fabric or have classified data.
- Separate devices into department, administrative, or other functional group.
- Reserve a path and its bandwidth from one port to another.

A zone is a named group of devices that can communicate with each other. Membership in a zone can be defined by switch module domain ID and port number, port Fibre Channel address, or by device worldwide name (WWN). Devices can communicate only with devices within the same zone. The switch module supports both hard and soft zones. The switch supports one zone set; that is, the active zone set. The active zone set determines the current fabric zoning.

A zoning database is maintained on each switch module consisting of the active zone set, all zones, and their membership. Table 2-1 describes the zoning database limits, excluding the active zone set. Refer to the *McDATA Switch Module Management Guide* for more information about zoning.

Table 2-1. Zoning Database Limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (1).
MaxZones	Maximum number of zones (2047).
MaxTotalMembers	Maximum number of zone members (10,000) that can be stored in the switch module's zoning database.
MaxZonesInZoneSets	Maximum number of zones that are components of the active zone set (2047), excluding the orphan zone set, that can be stored in the switch module's zoning database.
MaxMembersPerZone	Maximum number of members in a zone (10,000)

Soft Zones

Soft zoning divides the fabric for purposes of controlling device discovery. Devices in the same soft zone automatically discover and communicate freely with all other members of the same zone. The soft zone boundary is not secure; traffic across soft zones can occur if addressed correctly. The following rules apply to soft zones:

- Soft zones that include members from multiple switches need not include the ports of the inter-switch links.
- Soft zone boundaries yield to ACL zone boundaries.
- Soft zones can overlap; that is, a port can be a member of more than one soft zone.
- Membership can be defined by Fibre Channel address, domain ID and port number, or port worldwide name.
- Soft zoning supports FL_Ports and F_Ports.

Access Control List Hard Zones

Access Control List (ACL) zoning divides the fabric for purposes of controlling discovery and inbound traffic. ACL zoning is a type of hard zoning that is hardware enforced. This type of zoning is useful for controlling access to certain devices without totally isolating them from the fabric. Members can communicate with each other and transmit outside the ACL zone, but cannot receive inbound traffic from outside the zone. The following rules apply to ACL zones:

- The ACL zone boundary is secure against inbound traffic.
- ACL zones can overlap; that is, a port can be a member of more than one ACL zone.
- ACL zones that include members from multiple switches need not include the ports of the inter-switch links.
- ACL zone boundaries supersede soft zone boundaries.
- Membership can be defined only by domain ID and port number. A switch module port can be a member of multiple ACL zones whose combined membership does not exceed 64.

Performance

The switch module supports class 2 and class 3 Fibre Channel service with a maximum frame size of 2148 bytes at transmission rates of 1-Gbps, 2-Gbps, or 4-Gbps. An external port adapts its transmission speed to match that of the device to which it is connected prior to login when the connected device powers up. Related performance characteristics include the following:

- Distance
- Bandwidth
- Latency

Distance

Consider the physical distribution of devices and switches in the fabric. Choose SFP transceivers that are compatible with the cable type, distance, Fibre Channel revision level, and the device host bus adapter. Refer to Specifications for more information about cable types and transceivers.

Each Fibre Channel port is supported by a data buffer with a 16 credit capacity; that is, 16 maximum sized frames. For fibre optic cables, this enables full bandwidth over the following approximate distances:

- 26 kilometers at 1-Gbps (0.6 credits/Km)
- 13 kilometers at 2-Gbps (1.2 credits/Km)
- 6 kilometers at 4-Gbps (2.4 credits/Km)

Beyond these distances, however, there is some loss of efficiency because the transmitting port must wait for an acknowledgement before sending the next frame.

Longer distances can be spanned at full bandwidth by extending credits to G_Ports, F_Ports, and E_Ports. Each port can donate 15 credits to a pool from which a recipient port can borrow. The recipient port also loses a credit in the process. For example, you can configure a recipient port to borrow 15 credits from one donor port for a total of 30 credits (15+15=30). This will support communication over the following approximate distances:

- 50 Km at 1-Gbps (30÷0.6)
- 25 Km at 2-Gbps (30÷1.2)
- 12 Km at 4-Gbps (30÷2.4)

You can configure recipient and donor ports using the Set Config command. Refer to the *McDATA 4416 Command Line Interface Guide* for information about the Set Config command.

Bandwidth

Bandwidth is a measure of the volume of data that can be transmitted at a given transmission rate. A Fibre Channel port can transmit or receive at nominal rates of 1-Gbps, 2-Gbps, or 4-Gbps depending on the device to which it is connected. This corresponds to actual bandwidth values of 106 MB, 212 MB, and 425 MB respectively. Multiple source ports can transmit to the same destination port if the destination bandwidth is greater than or equal to the combined source bandwidth. For example, two 1-Gbps source ports can transmit to one 2-Gbps destination port. Similarly, one source port can feed multiple destination ports if the combined destination bandwidth is greater than or equal to the source bandwidth.

In multiple chassis fabrics, each link between chassis contributes 106, 212, or 425 MB of bandwidth between those chassis depending on the speed of the link. When additional bandwidth is needed between devices, increase the number of links between the connecting switches. The switch module guarantees in-order-delivery with any number of links between chassis.

Latency

Latency is a measure of how fast a frame travels from one port to another. The factors that affect latency include transmission rate and the source/destination port relationship as shown in Table 2-2.

Table 2-2. Port-to-Port Latency

	Destination Rate			
Source Rate	Gbps	1	2	4
	1	< 0.6 µsec	< 0.8 µsec[1]	< 0.8 µsec[1]
	2	< 0.5 µsec	< 0.4 µsec	< 0.4 µsec[1]
	4	< 0.4 µsec	< 0.3 µsec	< 0.3 µsec

[1] Based on minimum frame size of 36 bytes. Latency increases for larger frame sizes.

Multiple Chassis Fabrics

By connecting switches together you can expand the number of available ports for devices. Each switch in the fabric is identified by a unique domain ID, and the fabric can automatically resolve domain ID conflicts. Because the Fibre Channel ports are self-configuring, you can connect switches together in a wide variety of topologies.

Optimizing Device Performance

When choosing a topology for a multiple chassis fabric, you should also consider the locality of your server and storage devices and the performance requirements of your application. Storage applications such as video distribution, medical record storage/retrieval or real-time data acquisition can have specific latency or bandwidth requirements.

The switch module provides the lowest latency of any product in its class. Refer to "Performance" on page 2-4 for information about latency. However, the highest performance is achieved on Fibre Channel switches by keeping traffic within a single switch instead of relying on ISLs. Therefore, for optimal device performance, place devices on the same switch module under the following conditions:

- Heavy I/O traffic between specific server and storage devices.
- Distinct speed mismatch between devices

Domain ID, Principal Priority, and Domain ID Lock

The following switch configuration settings affect multiple chassis fabrics:

- Domain ID
- Principal priority
- Domain ID lock

The domain ID is a unique number that identifies each switch in a fabric. The valid domain ID range depends on the interoperability mode:

- When the interoperability mode is Standard, the domain ID can be 97–127.
- When the interoperability mode is McDATA Fabric Mode, the domain ID can be 1–31.

The principal priority is a number (1–255) that determines the principal switch which manages domain ID assignments for the fabric. The switch with the highest principal priority (1 is high, 255 is low) becomes the principal switch. If the principal priority is the same for all switches in a fabric, the switch with the lowest WWN becomes the principal switch.

The domain ID lock allows (False) or prevents (True) the reassignment of the domain ID on that switch. Switches come from the factory with the domain ID set to 1, the domain ID lock set to False, and the principal priority set to 254. Refer to the *McDATA Switch Module Management Guide* for information about changing the domain ID and domain ID lock using McDATA Embedded Web Server. Refer to the Set Config command in the *McDATA 4416 Command Line Interface Guide* for information about changing the default domain ID, domain ID lock, and principal priority parameters.

An unresolved domain ID conflict means that the switch with the higher WWN will isolate as a separate fabric, and the Logged-In LEDs on both switches will flash green to show the affected ports. If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain ID conflict occurs, the new switch will isolate as a separate fabric. However, you can remedy this by resetting the new switch or taking it offline then back online. The principal switch will reassign the domain ID and the switch will join the fabric.

NOTE: Domain ID reassignment is not reflected in zoning that is defined by domain ID/port number pair or Fibre Channel address. You must reconfigure zones that are affected by domain ID reassignment. To prevent zoning definitions from becoming invalid under these conditions, lock the domain IDs using McDATA Embedded Web Server, McDATA Element Manager, or the Set Config Switch command.

Switch Module Services

You can configure your switch module to suit the demands of your environment by enabling or disabling a variety of switch services. Familiarize yourself with the following switch services and determine which ones you need:

- **Telnet**: Provides for the management of the switch over a Telnet connection. Disabling this service is not recommended. The default is enabled.
- **Secure Shell (SSH)**: Provides for secure remote connections to the switch using SSH. Your workstation must also use an SSH client. The default is disabled.
- **Switch Management**: Provides for out-of-band management of SNMP and CIM. If this service is disabled, the switch can only be managed inband or through the serial port. The default is enabled.
- **Inband Management**: Provides for the management of the switch over an inter-switch link using McDATA Embedded Web Server, McDATA Element Manager, SNMP, or management server. If you disable inband management, you can no longer communicate with that switch by means other than a direct Ethernet or serial connection.The default is enabled.

- **Secure Socket Layer (SSL)**: Provides for secure SSL connections for McDATA Embedded Web Server, McDATA Element Manager, and CIM. This service must be enabled to authenticate users through a RADIUS server when using McDATA Embedded Web Server or McDATA Element Manager. To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation. Enabling SSL automatically creates a security certificate on the switch. The default is enabled.
- **Embedded GUI**: Provides for access to the McDATA Embedded Web Server and McDATA Element Manager. McDATA Element Manager enables you to manage a switch module through EFCM. The default is enabled.

NOTE: McDATA Element Manager is available through EFCM only with the Element Manager PFE key. Refer to *McDATA Switch Module Management Guide* for information about installing a PFE key. For additional McDATA PFE keys, please contact your McDATA representative or visit the web site at www.mcdata.com.

- **Simple Network Management Protocol (SNMP)**: Provides for the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). Security consists of a read community string and a write community string that serve as passwords that control read and write access to the switch. These strings are set at the factory to these well-known defaults and should be changed if SNMP is to be enabled. Otherwise, you risk unwanted access to the switch. The default is enabled.
- **Network Time Protocol (NTP)**: Provides for the synchronizing of switch and workstation dates and times with an NTP server. This helps to prevent invalid SSL certificates and timestamp confusion in the event log. The default is disabled.
- **Common Information Model (CIM)**: Provides for the management of the switch through third-party applications that use CIM. The default is enabled.
- **File Transfer Protocol (FTP)**: Provides for transferring files rapidly between the workstation and the switch using FTP. The default is enabled.
- **Management Server (MS)**: Enables or disables the management of the switch through third-party applications that use GS-3 Management Server. The default is disabled.

Fabric Security

An effective security profile begins with a security policy that states the requirements. A threat analysis is needed to define the plan of action followed by an implementation that meets the security policy requirements. Internet portals, such as remote access and E-mail, usually present the greatest threats. Fabric security should also be considered in defining the security policy.

Most fabrics are located at a single site and are protected by physical security, such as key-code locked computer rooms. For these cases, security methods such as user passwords and zoning are satisfactory.

Fabric security is needed when security policy requirements are more demanding: for example, when fabrics span multiple locations and traditional physical protection is insufficient to protect the IT infrastructure. Another benefit of fabric security is that it creates a structure that helps prevent unintended changes to the fabric.

Fabric security consists of the following:

- Connection Security
- Device Security
- User Account Security

Connection Security

Connection security provides an encrypted data path for switch management methods. The switch supports the Secure Shell (SSH) protocol for the command line interface and the Secure Socket Layer (SSL) protocol for management applications such as McDATA Embedded Web Server, McDATA Element Manager, and Common Information Module (CIM).

The SSL handshake process between the workstation and the switch involves the exchanging of certificates. These certificates contain the public and private keys that define the encryption. When the SSL service is enabled, a certificate is automatically created on the switch. The workstation validates the switch certificate by comparing the workstation date and time to the switch certificate creation date and time. For this reason, it is important to synchronize the workstation and switch with the same date, time, and time zone. The switch certificate is valid 24 hours before its creation date and 365 days after its creation date. If the certificate should become invalid, refer to the Create command in the *McDATA 4416 Command Line Interface Guide* for information about creating a certificate.

Consider your requirements for connection security: for the command line interface (SSH), management applications such as McDATA Embedded Web Server (SSL), or both. If SSL connection security is required, also consider using the Network Time Protocol (NTP) to synchronize workstations and switches.

- Refer to System keyword of the Set Setup command in the *McDATA 4416 Command Line Interface Guide* for information about enabling the NTP client on the switch and configuring the NTP server.
- Refer to the Set command in the *McDATA 4416 Command Line Interface Guide* for information about setting the time zone.

Device Security

NOTE: Device security is available only with the SANtegrity Enhanced PFE key. Refer to *McDATA Switch Module Management Guide* for information about installing a PFE key. For additional McDATA PFE keys, please contact your McDATA representative or visit the web site at www.mcdata.com.

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or devices issuing management server commands. Device security is configured through the use of security sets and groups. A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS). A security set is a set of up to three groups with no more than one of each group type. The security configuration is made up of all security sets on the switch. The security database has the following limits:

- Maximum number of security sets is 4.
- Maximum number of groups is 16.
- Maximum number of members in a group is 1000.
- Maximum total number of group members is 1000.

In addition to authorization, the switch can be configured to require authentication to validate the identity of the connecting switch, device, or host. Authentication can be performed locally using the switch's security database, or remotely using a Remote Dial-In User Service (RADIUS) server such as Microsoft® RADIUS. With a RADIUS server, the security database for the entire fabric resides on the server. In this way, the security database can be managed centrally, rather than on each switch module. You can configure up to five RADIUS servers to provide failover.

You can configure the RADIUS server to authenticate just the switch module or both the switch module and the initiator device if the device supports authentication. When using a RADIUS server, every switch in the fabric must have a network connection. A RADIUS server can also be configured to authenticate user accounts as described in "User Account Security" on page 2-11. A secure connection is required to authenticate user logins with a RADIUS server. Refer to "Connection Security" on page 2-9 for more information.

Consider the devices, switches, and management agents and evaluate the need for authorization and authentication. Also consider whether the security database is to distributed on the switches or centralized on a RADIUS server and how many servers to configure.

User Account Security

User account security consists of the administration of account names, passwords, expiration date, and authority level. If an account has Admin authority, all management tasks can be performed by that account in McDATA Embedded Web Server, McDATA Element Manager, and the Telnet command line interface. Otherwise only monitoring tasks are available. The default account name, Admin, is the only account that can create or change account names and passwords. Account names and passwords are always required when connecting to a switch.

Authentication of the user account and password can be performed locally using the switch's user account database or it can be done remotely using a RADIUS server such as Microsoft® RADIUS. Authenticating user logins on a RADIUS server requires a secure management connection to the switch. Refer to "Connection Security" on page 2-9 for information about securing the management connection. A RADIUS server can also be used to authenticate devices and other switches as described in "Device Security" on page 2-10.

Consider your management needs and determine the number of user accounts, their authority needs, and expiration dates. Also consider the advantages of centralizing user administration and authentication on a RADIUS server.

NOTE: If the same user account exists on a switch and its RADIUS server, that user can login with either password, but the authority and account expiration will always come from the switch database.

Fabric Management

The McDATA Embedded Web Server application, McDATA Element Manager application, and CLI reside on the switch. These applications provide for the configuration, control, and maintenance of one fabric using McDATA Embedded Web Server, or one switch using McDATA Element Manager or the CLI. McDATA Element Manager requires the Element Manager PFE key and must be launched from EFCM. Supported workstation platforms include Windows and Linux.

Consider how many fabrics will be managed, how many management workstations are needed, and whether the fabrics will be managed with the McDATA Embedded Web Server, McDATA Element Manager, or the CLI.

A switch supports a combined maximum of 19 logins reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for McDATA Embedded Web Server, McDATA Element Manager, Telnet. Additional logins will be refused.

Notes

3 Installation

This section describes how to install and configure the McDATA 4416 switch module. It also describes how to load new firmware and how to recover a disabled switch module.

Site Requirements

Consider the following items when installing a McDATA 4416 switch module:

- Fabric Management Workstation
- Environmental Conditions

Fabric Management Workstation

The requirements for fabric management workstations running McDATA Embedded Web Server are described in Table 3-1:

Table 3-1. Workstation Requirements

Component	Requirement
Operating System	• Windows 2000/2003 • Linux® Red Hat® EL 3.x, 4.x
Memory	256 MB or more
Processor	500 MHz or faster
Hardware	CD-ROM drive, RJ-45 Ethernet port
Internet Browser	Microsoft® Internet Explorer® 5.0 and later Netscape Navigator® 4.72 and later Mozilla™ 1.02 and later Java 2 Runtime Environment to support the McDATA Embedded Web Server and McDATA Element Manager.

Telnet workstations require an RJ-45 Ethernet port and an operating system with a Telnet client.

Environmental Conditions

Consider the factors that affect the climate in your facility such as equipment heat dissipation and ventilation. The switch requires the following operating conditions:

- Operating temperature range: 5 – 40°C (41 – 104°F)
- Relative humidity: 5 – 90%, non-condensing

Installing a Switch

Installing a McDATA 4416 switch module involves the following steps:

1. Install SFP Transceivers
2. Mount the Switch Module in the Server Chassis
3. Connect the Management Workstation to the Switch Module
4. Start McDATA Embedded Web Server or McDATA Element Manager
5. Configure the Switch Module
6. Cable Devices to the Switch

Install SFP Transceivers

The switch module has been validated with transceivers that support a variety of interconnection media. To install a transceiver, insert the transceiver into the port and gently press until it snaps in place. The transceiver will fit only one way. If the transceiver does not install under gentle pressure, turn it over and try again.

NOTE: If you have installed the Port Activation PFE key, all six external ports are enabled. Otherwise, only ports 10–13 are enabled.

To remove a transceiver, gently press the transceiver into the port to release the tension, then pull on the release tab or lever and remove the transceiver. Different transceiver manufacturers have different release mechanisms. Consult the documentation for your transceiver.

Mount the Switch Module in the Server Chassis

McDATA 4416 switch modules are installed in server chassis I/O module slots 3 and 4 as shown in Figure 3-1. For a single switch module installation, use I/O module slot 3. Do not attempt to install the McDATA 4416 switch module in any other I/O module slots.

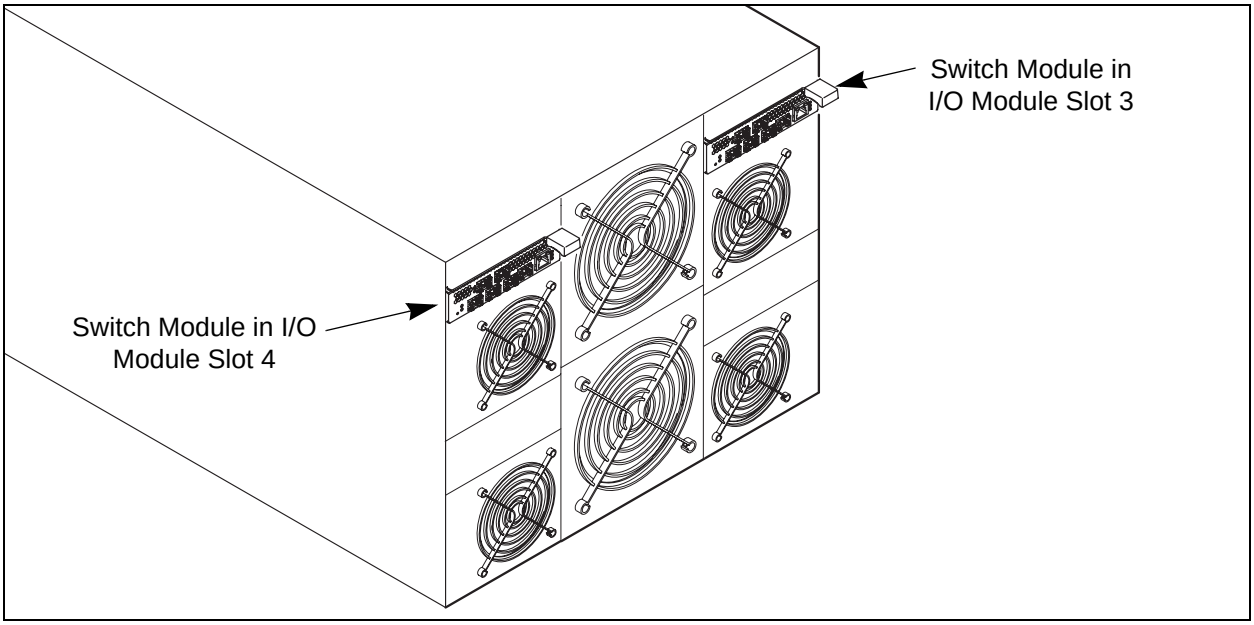

Figure 3-1. Mounting the Switch Module in the Server Chassis

To insert the McDATA 4416 switch module, do the following:

1. Verify that chassis I/O module slots 3 and 4 are empty.
2. Gripping from the top and bottom of the release latch, gently squeeze the latch to free the insertion arm.
3. Swing the insertion arm out (away from the chassis) until it is completely open.
4. Slide the switch module into the open I/O module slot.
5. Push the insertion arm gently toward the chassis until it is completely closed and the switch module is firmly seated.

CAUTION

Do not force the arm closed. Doing so could cause damage. Instead, if the switch module does not close easily, gently remove the switch module and reinsert it.

When energized, the switch module responds in the following sequence:

1. The switch module LEDs (Identifier, Input Power, System Fault) illuminate followed by all port Logged-In LEDs.
2. After a couple seconds the System Fault LED is extinguished while the Input Power LED remains illuminated.
3. After approximately one minute, the POST executes.
4. After about another minute, the POST is complete, all LEDs are extinguished except the Input Power LED. The Input Power LED remains illuminated indicating that the switch logic circuitry is receiving DC voltage. If not, contact your authorized maintenance provider.

Connect the Management Workstation to the Switch Module

Connect the management workstation to the switch module in the following ways:

- Indirect Ethernet connection from the management workstation to the switch module RJ-45 Ethernet connector through an Ethernet switch or a hub. This requires a 10/100 Base-T Ethernet straight cable as shown in Figure 3-2. With this method, you can manage the switch module with the McDATA Embedded Web Server application or Command Line Interface.
- Direct Ethernet connection from the management workstation to the switch module RJ-45 Ethernet connector. This requires a 10/100 Base-T Ethernet cross-over cable as shown in Figure 3-2. With this method, you can manage the switch module with the McDATA Embedded Web Server application or Command Line Interface.

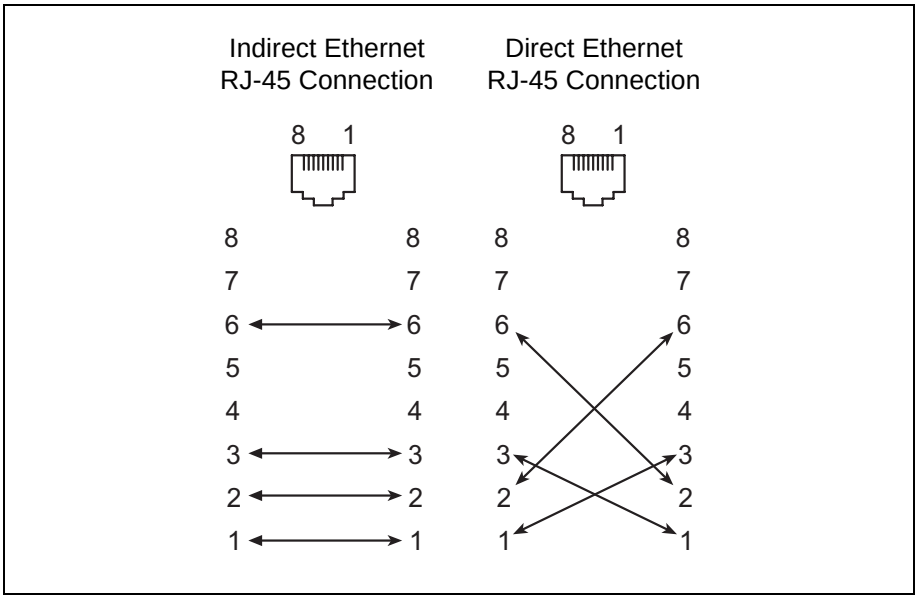

Figure 3-2. Ethernet Cable Connections

The default IP address of a new switch module is 10.0.0.1. Many management workstations are not configured to communicate with the 10.0.0 subnet. Use the McDATA Embedded Web Server Configuration Wizard to set the IP address of a new switch without re-configuring the management workstation.

To establish an Ethernet connection, do the following:

1. Connect a 10/100 Base-T Ethernet cross-over cable from an RJ-45 port on the management workstation directly to the RJ-45 Ethernet port; or a 10/100 Base-T straight cable indirectly over an Ethernet network.
2. Open a command line window.
3. Open a Telnet session by entering the following command with the switch IP address. The default IP address is 10.0.0.1

   ```
   telnet 10.0.0.1
   ```

4. Log in to the switch. The default account name and password are (admin, password).

   ```
   Switch Login: admin
   Password: ********
   ```

Start McDATA Embedded Web Server or McDATA Element Manager

You can manage the switch using McDATA Embedded Web Server or McDATA Element Manager through EFCM.

- To start the McDATA Embedded Web Server application for the first time, enter the switch IP address in an internet browser. If your workstation does not have the Java 2 Run Time Environment program, you will be prompted to download it.
- Open McDATA Element Manager from EFCM. In EFCM, add the switch IP address to the discovery list. Locate and double click the switch in the fabric map to open. You can also select the switch and select **Element Manager (HTML)** from the application list. Refer to your EFCM documentation for information about using EFCM.

In the Initial Start dialog, click the **Open Configuration Wizard** button. When you power up the switch, the Configuration Wizard will recognize the switch and lead you through the configuration process.

Configure the Switch Module

You can configure the switch using the McDATA Embedded Web Server application, the McDATA Element Manager, or the command line interface. Using McDATA Embedded Web Server or McDATA Element Manager, click the **Open Configuration Wizard** radio button in the Initial Start dialog, then click the **Proceed** button. The Configuration wizard explains and prompts you for the following configuration information:

- Archive template file
- Switch domain ID
- Domain ID Lock
- Switch name
- Permanent IP address
- Permanent subnet mask
- Permanent gateway address
- Permanent network discovery method
- Date and time
- Admin account password
- Create a configuration archive?

NOTE: Refer to the Reset command in the *McDATA 4416 Command Line Interface Guide* for information about configuration default values.

To configure the switch using the command line interface, do the following:

1. Open a Telnet session with the default switch IP address and log in to the switch with default account name and password (admin/password).

   ```
   telnet 10.0.0.1
   Switch Login: admin
   Password:     *******
   ```

2. Open an admin session and enter the Set Setup System command. Enter the values you want for switch IP address (Eth0NetworkAddress) and the network mask (Eth0NetworkMask). Refer to the *McDATA 4416 Command Line Interface Guide* for more information about this command.

   ```
   DFCSM4Gb #> admin start
   DFCSM4Gb (admin) #> set setup system
   ```

3. Open a Config Edit session and use the Set Config command to modify the switch configuration. Refer to the *McDATA 4416 Command Line Interface Guide* for more information about these commands.

Cable Devices to the Switch

Connect cables to the SFP transceivers and their corresponding devices, and then energize the devices. Device host bus adapters can have SFP (or SFF) transceivers or GigaBit Interface Converters (GBIC). LC-type duplex fiber optic cable connectors are designed for SFP transceivers, while SC-type connectors are designed for GBICs. Duplex cable connectors are keyed to ensure proper orientation. Choose the fiber optic cable with the connector combination that matches the device host bus adapter.

GL_Ports self configure as FL_Ports when connected to loop of public devices or F_Ports when connected to a single device. G_Ports self configure as F_Ports when connected to single public devices. Both GL_Ports and G_Ports self configure as E_Ports when connected to another switch.

Install Firmware

The switch module comes with current firmware installed. You can upgrade the firmware from the management workstation as new firmware becomes available. You can use the McDATA Embedded Web Server application, the McDATA Element Manager, or the CLI to install new firmware.

You can load and activate version 5.2.3 firmware on an operating switch without disrupting data traffic or having to re-initialize attached devices. If you attempt to perform a non-disruptive activation without satisfying the following conditions, the switch will perform a disruptive activation:

- The current firmware version is a 5.2.3 version that precedes the upgrade version.
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, and switch configuration changes.
- No port in the fabric is in the diagnostic state.
- No zoning changes are being made in the fabric.
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.

Ports that are stable when the non-disruptive activation begins, then change states, will be reset. When the non-disruptive activation is complete, McDATA Embedded Web Server or McDATA Element Manager sessions reconnect automatically. However, Telnet sessions must be restarted manually.

Using McDATA Embedded Web Server or McDATA Element Manager to Install Firmware

To install firmware using McDATA Embedded Web Server or McDATA Element Manager, do the following:

1. In the faceplate display, open the Switch menu and select **Load Firmware**.
2. In the Firmware Upload window, click the **Select** button to browse and select the firmware file to be uploaded.
3. Click the **Start** button to begin the firmware load process. You will be shown a message warning you that the switch will be reset to activate the firmware.
4. Click the **OK** button to continue firmware installation or click the **Cancel** button to cancel the firmware installation. The switch will attempt a hot reset, if possible, to activate the firmware without disrupting data traffic. During a non-disruptive activation, all Logged-In LEDs are extinguished for several seconds. If a non-disruptive activation is not possible, the application gives you the opportunity to reset the switch module and perform a disruptive activation.

Using the CLI to Install Firmware

To install firmware using the CLI when a File Transfer Protocol (FTP) server is present on the management workstation, use the Firmware Install command. Refer to the *McDATA 4416 Command Line Interface Guide* for information about this command.

NOTE: Installing firmware using the Firmware Install command is disruptive to the fabric. To perform a non-disruptive firmware installation refer to the Image command in the *McDATA 4416 Command Line Interface Guide*.

1. Enter the following command to download the firmware from a remote host to the switch, install the firmware, then reset the switch to activate the firmware.

   ```
   DFCSM4Gb (admin) #> firmware install

   Warning: Continuing with this action will terminate all
   management sessions, including any Telnet sessions. When the
   firmware activation is complete, you may log in to the switch
   again.

   Do you want to continue? [y/n]: y

   Press 'q' and the ENTER key to abort this command.
   ```

2. Enter your account name on the remote host and the IP address of the remote host. When prompted for the source file name, enter the path for the firmware image file.

   ```
   User Account : johndoe
   IP Address : 10.20.20.200
   Source Filename : 5.2.3.x.xx.xx_mpc
   ```

3. When prompted to install the new firmware, enter Yes to continue or No to cancel. This is the last opportunity to cancel.

   ```
   About to install image. Do you want to continue? [y/n] y
   Connected to 10.20.20.200 (10.20.20.200).

   220 localhost.localdomain FTP server (Version wu-2.6.1-18)
   ready.
   ```

4. Enter the password for your account name. The firmware will now be downloaded from the remote host to the switch module, installed, and activated.

   ```
   331 Password required for johndoe.
   Password:******
   230 User johndoe logged in.
   ```

Notes

4 Troubleshooting

Diagnostic information about the switch is available through the switch module LEDs and the external port LEDs. Diagnostic information is also available through the McDATA Embedded Web Server and CLI event logs and error displays.

The switch performs a series of tests as part of its power-up procedure. The POST diagnostic program performs the following tests:

- Checksum tests on the boot firmware in PROM and the switch firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the ASIC

During the POST, the switch logs any errors encountered. Some POST errors are critical, others are not. The switch uses the System Fault LED and the Logged-In LED to indicate switch and port status. A critical error disables the switch so that it will not operate. A non-critical error allows the switch to operate, but disables the ports that have errors.

Input Power LED Is Extinguished

The Input Power LED illuminates to indicate that the switch logic circuitry is receiving proper voltages. If the Input Power LED is extinguished, contact your authorized maintenance provider.

System Fault LED is Illuminated

The System Fault LED illuminates to indicate that the switch module logic circuitry is overheating or that a POST error has occurred. If the System Fault LED illuminates, contact your authorized maintenance provider.

Logged-In LED Indications

Port diagnostics are indicated by the Logged-In LED for each port as shown in Figure 4-1.

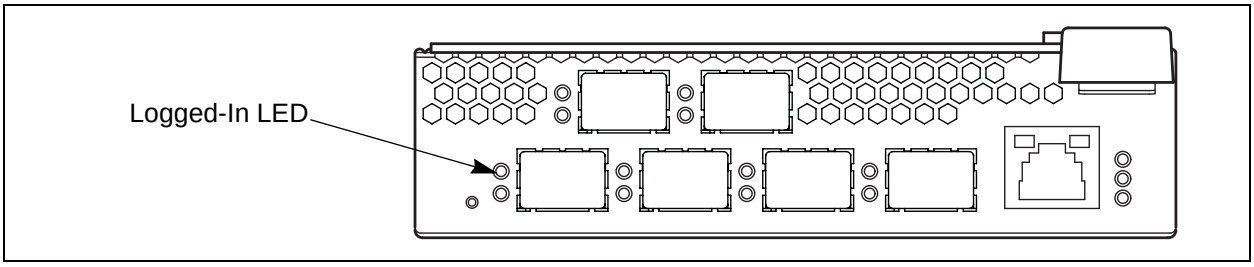

Figure 4-1. Logged-In LED

The Logged-In LED has three indications:

- Continuous illumination: A device is logged in to the port.
- Flashing once per second: A device is logging in to the port.
- Flashing twice per second: The port is down, offline, or an error has occurred.

If a Logged-In LED is flashing twice per second, review the event browser for alarm messages regarding the affected port. You can also inspect the alarm log using the Show Alarm command. If there is an error, alarm messages may point to one or more of the following conditions:

- E_Port Isolation
- Excessive Port Errors

E_Port Isolation

A Logged-In LED error indication is often the result of E_Port isolation. An isolated E_Port is indicated by a red link in the McDATA Embedded Web Server topology display. E_Port isolation can be caused by the following:

- Security failure
- FL_Port is connected to another switch
- Conflicting domain IDs
- Conflicting timeout values
- Conflicting zone membership between active zone sets

Refer to the *McDATA Switch Module Management Guide* for information about how to change domain IDs, timeout values, and edit zoning.

Review the event browser and do the following to diagnose and correct an isolated E_Port:

1. Does the event browser show an alarm about an invalid attach on the affected port?
   - Yes - Review the ISL group in the active security set to ensure that the membership includes the necessary ports and that the secrets on all switches are correct.
   - No - Continue.
2. Does the event browser show a repeating alarm about an unsupported E_Port command on the affected port?
   - Yes - The port is configured as an FL_Port and connected to another switch. Correct the port connection or the port type.
   - No - Continue.
3. Display the fabric domain IDs using the Show Domains command or the Switch data tab in the McDATA Embedded Web Server topology display. Are all domain IDs in the fabric unique?
   - Yes - Continue.
   - No - Correct the domain IDs on the offending switches using the Set Config Switch command or the McDATA Embedded Web Server Switch Properties window. Reset the port. If the condition remains, continue.
4. Compare the RA_TOV and ED_TOV timeout values for all switches in the fabric using the Show Config Switch command or the Switch data tab of the McDATA Embedded Web Server topology display. Is each timeout value the same on every switch?
   - Yes - Continue.
   - No - Correct the timeout values on the offending switches using the Set Config Switch command or the McDATA Embedded Web Server Switch Properties dialog. Reset the port. If the condition remains, continue.
5. Display the active zone set on each switch using the Zoning Active command or the Active Zoneset tab of the McDATA Embedded Web Server topology display. Compare the zone membership between the two active zone sets. Are they the same?
   - Yes - Contact your authorized maintenance provider.
   - No - Deactivate one of the active zone sets or edit the conflicting zones so that their membership is the same. Reset the port. If the condition remains, contact your authorized maintenance provider.

NOTE: This can be caused by merging two fabrics whose active zone sets have two zones with the same name, but different membership.

Excessive Port Errors

The switch can monitor a set of port errors and generates alarms based on user-defined sample windows and thresholds. These port errors include the following:

- CRC errors
- Decode errors
- ISL connection count
- Login errors
- Logout errors
- Loss-of-signal errors

Port threshold alarm monitoring is disabled by default. Refer to the *McDATA Switch Module Management Guide* for information about managing port threshold alarms.

If the count for any of these errors exceeds the rising trigger for three consecutive sample windows, the switch generates an alarm and disables the affected port, changing its operational state to "down". Port errors can be caused by the following:

- Triggers are too low or the sample window is too small
- Faulty Fibre Channel port cable
- Faulty SFP
- Faulty port
- Fault device or HBA

Review the event browser to determine if excessive port errors are responsible for disabling the port. Look for a message that mentions one of the monitored error types indicating that the port has been disabled, then do the following:

1. Examine the alarm configuration for the associated error using the Show Config Threshold command or the McDATA Embedded Web Server application. Refer to the *McDATA 4416 Command Line Interface Guide* for information about this command. Are the thresholds and sample window correct?
   - Yes - Continue
   - No - Correct the alarm configuration. If the condition remains, continue.
2. Reset the port, then perform an external port loopback test to validate the port and the SFP. Refer to the *McDATA Switch Module Management Guide* for information about testing ports. Does the port pass the test?
   - Yes - Continue
   - No - Replace the SFP and repeat the test. If the port does not pass the test, contact your authorized maintenance provider. Otherwise continue.

3. Replace the Fibre Channel port cable. Is the problem corrected?
   - Yes - Complete.
   - No - Continue.
4. Inspect the device to which the affected port is connected and confirm that the device and its HBA are working properly. Make repairs and corrections as needed. If the condition remains, contact your authorized maintenance provider.

Recovering a Switch Module

A switch can become inoperable or unmanageable for the following reasons:

- Firmware becomes corrupt
- IP address is lost
- Switch configuration becomes corrupt
- Forgotten password

In these specific cases, you can recover the switch using maintenance mode. Maintenance mode temporarily returns the switch IP address to 10.0.0.1 and provides opportunities to do the following:

- Unpack a firmware image file
- Restore the network configuration parameters to the default values
- Remove all user accounts and restore the Admin account name password to the default.
- Copy the log file
- Restore factory defaults for all but user accounts and zoning
- Restore all switch configuration parameters to the factory default values
- Reset the switch
- Update the system boot loader

To recover a switch, do the following:

1. Place the switch in maintenance mode. Press and hold the Maintenance button with a pointed tool for 2–7 seconds.
2. Allow one minute for the switch to complete its tests. When the switch is in maintenance mode, all switch module LEDs are extinguished.
3. Establish a Telnet session with the switch using the maintenance mode IP address 10.0.0.1.
4. Enter the maintenance mode account name and password (prom, prom), and press the Enter key.

```
Switch login: prom
Password:xxxx
```

5. The maintenance menu displays several recovery options. To select a switch recovery option, press the corresponding number (displayed in option: field) on the keyboard and press the Enter key.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset User Accounts to Default
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
8)  Update Boot Loader
Option:
```

These options and their use are described in the following subsections.

Maintenance – Exit

This option closes the current login session. To log in again, enter the maintenance mode account name and password (prom, prom). To return to normal operation, momentarily press and release the Maintenance button or power cycle the switch module.

Maintenance – Image Unpack

This option unpacks and installs new firmware when the current firmware has become corrupt. Before using this option, you must load the new firmware image file onto the switch. The steps to install new firmware using this option are as follows:

1. Place the switch in maintenance mode. Refer to the procedure for maintenance mode in "Recovering a Switch Module" on page 4-5.
2. Use the Image command to load a new firmware image file onto the switch. Refer to the *McDATA 4416 Command Line Interface Guide* for an example of using the Image command. Close the FTP session.
3. Establish a Telnet session with the switch using the default IP address 10.0.0.1.

```
telnet 10.0.0.1
```

4. Enter the maintenance mode account name and password (prom, prom), and press the Enter key.

```
Switch login: prom
Password:xxxx
```

5. Select option 1 from the maintenance menu. When prompted for a file name prompt, enter the firmware image file name.

```
Image filename: filename
Unpacking 'filename', please wait...
Unpackage successful.
```

6. Select option 7 to reset the switch and exit maintenance mode.

Maintenance – Reset Network Config

This option resets the network properties to the factory default values and saves them on the switch. Refer to the Reset command in the *McDATA 4416 Command Line Interface Guide* for the default network configuration values.

Maintenance – Reset User Accounts to Default

This option restores the password for the Admin account name to the default (password) and removes all other user accounts from the switch.

Maintenance – Copy Log Files

This option copies all log file buffers to a file on the switch named *logfile*. You can use FTP to download this file to the management workstation. You must download the logfile before resetting the switch.

Maintenance – Remove Switch Config

This option deletes all configurations from the switch except the default configuration. This restores switch configuration parameters to the factory defaults. Refer to Reset command in the *McDATA 4416 Command Line Interface Guide* for factory default values.

Maintenance – Remake Filesystem

In the event of a loss of power, the switch configuration may become corrupt. The file system on which the configuration is stored must be re-created. This option resets the switch to the factory default values including user accounts and zoning. Refer to the Reset command in the *McDATA 4416 Command Line Interface Guide* for the factory default values.

CAUTION

If you choose the Remake Filesystem option, you will lose all changes made to the fabric configuration that involve that switch, such as password and zoning changes. You must then restore the switch from an archived configuration or reconfigure the portions of the fabric that involve the switch.

Maintenance – Reset Switch

This option closes the Telnet session, exits maintenance mode and reboots the switch using the current switch configuration. All unpacked firmware image files that reside on the switch are deleted.

Maintenance – Update Boot Loader

This option updates the system boot loader which loads the Linux kernel into memory. Use this option only at the direction of your authorized maintenance provider.

Notes

A

Specifications

This appendix contains the specifications for the McDATA 4416 switch module. Refer to Chapter 1 for the location of all connections, switches, controls, and components.

Fabric Specifications

Table A-1. Fabric Specifications

Specification	Description
Fibre Channel Protocols	FC-PH Rev. 4.3 FC-PH-2 FC-PH-3 FC-AL Rev 4.6 FC-AL-2 Rev 7.0 FC-FLA FC-GS FC-GS-2 FC-GS-3 FC-FG FC-Tape FC-VI FC-SW-2 Fibre Channel Element MIB RFC 2837 Fibre Alliance MIB Version 4.0
Fibre Channel Classes of Service	Classes 2 and 3
Modes of Operation	Fibre Channel Classes 2 and 3, connectionless
Port Types	G_Port, GL_Port F_Port, FL_Port E_Port
Port Characteristics	All ports are auto-discovering and self-configuring.
Number of Fibre Channel Ports	4 external ports (PFE upgrade to 6 ports) 8 internal ports (PFE upgrade to 10 ports)
Scalability	Maximum 31 switches

Table A-1. Fabric Specifications (Continued)

Specification	Description
Maximum User Ports	> 475,000 ports depending on configuration
Buffer Credits	16 buffer credits per port, ASIC embedded memory
Media Type	SFP optical transceiver, hot-pluggable
Fabric Port Speed	1.0625, 2.125, or 4.250 Gbps
Maximum Frame Size	2148 bytes (2112 byte payload)
System Processor	200 MHz Motorola® 8245 PowerPc®
Fabric Latency (intra-switch) 1-Gbps to 1-Gbps 2-Gbps to 2-Gbps 4-Gbps to 4-Gbps	 < 0.6 µsec < 0.4 µsec < 0.3 µsec
Bandwidth Point-to-Point Aggregate (single switch)	 106 MB, Full Duplex @ 1-Gbps 212 MB, Full Duplex @ 2-Gbps 425 MB, Full Duplex @ 4-Gbps Up to 6.8 GB, Full Duplex

Maintainability Specifications

Table A-2. Maintainability Specifications

Specification	Description
Diagnostics	Power-On Self Test (POST) tests all functional components except SFP transceivers. Port tests include online, internal, and external tests.
User Interface	LED indicators

Fabric Management Specifications

Table A-3. Fabric Management Specifications

Specification	Description
Management Methods	McDATA Embedded Web Server McDATA Element Manager[1] through EFCM Command Line Interface GS-3 Management Server SNMP FTP
Ethernet Connection	RJ-45 connector; 10/100 BASE-T cable
Switch Agent	Allows a network management station to obtain configuration values, traffic information, and failure data pertaining to the Fibre Channels using SNMP through the Ethernet interface.

[1] Requires the Element Manager PFE key.

Dimensional Specifications

Table A-4. Dimensional Specifications

Specification	Description
Width Height Depth	9.89" (251.2 mm) 1.27" (32.2 mm) 5.11" (129.8 mm)
Weight	2 .06 lbs (0.94 kg)

Electrical Specifications

Table A-5. Electrical Specifications

Specification	Description
Operating voltage	5 VDC; 12 VDC
Power source loading (maximum)	100 mA at 5 VDC 3.75 A at 12 VDC
Heat Output (maximum)	75 watts
Circuit Protection	Internally fused

Environmental Specifications

Table A-6. Environmental Specifications

Specification	Description
Temperature	
• Operating	5 to 40°C (41 to 104°F)
• Non-operating	-40 to 70°C (-40 to 158°F)
Humidity	
• Operating	5% to 90%, non-condensing
• Non-operating	5% to 93%, non-condensing
Altitude	
• Operating	0 to 3048m (0 to 10,000 feet)
• Non-operating	0 to 15,240m (0 to 50,000 feet)
Vibration	IEC 68-2
• Operating	5-500 Hz, random, 0.21 G rms, 10 minutes
• Non-operating	5-500 Hz, random, 2.09 G rms, 10 minutes
Shock	IEC 68-2
• Operating	4 g, 11ms, 20 repetitions
• Non-operating	30g, 292 ips, 3 repetitions, 3 axis

Regulatory Certifications

Table A-7. Regulatory Certifications

Certification	Description
Safety Standards	UL60950:2000 CSA 22.2 No. 60950-00 (Canada) EN60950:2000 (EC) CB Scheme-IEC 60950:1999
Emissions Standards	FCC Part 15B Class A ICES-03 Issue 3 VCCI Class A ITE CISPR 22, Class A EN 55022, Class A
Voltage Fluctuations.....	EN 61000-3-3
Harmonics.....	EN 61000-3-2
Immunity	EN 55024:1998
Marking	FCC Part 15 UL_{US} (United States) TUV_{US} (United States) cUL (Canada) cTUV (Canada) TUV Europe (Germany) VCCI CE

Notes

Glossary

A

Access Control List Zone — Access Control List zoning divides the fabric for purposes of controlling discovery and inbound traffic.

Active Zone Set — The zone set that defines the current zoning for the fabric.

Active Firmware — The firmware image on the switch that is in use.

Activity LED — A port LED that indicates when frames are entering or leaving the port.

Administrative State — State that determines the operating state of the port, I/O blade, or switch. The configured administrative state is stored in the switch configuration. The configured administrative state can be temporarily overridden using the command line interface.

Alarm — A message generated by the switch that specifically requests attention. Alarms are generated by several switch processes. Some alarms can be configured.

AL_PA — Arbitrated Loop Physical Address

Arbitrated Loop — A Fibre Channel topology where ports use arbitration to establish a point-to-point circuit.

Arbitrated Loop Physical Address (AL_PA) — A unique one-byte value assigned during loop initialization to each NL_Port on a loop.

ASIC — Application Specific Integrated Circuit. A chip designed for a specific applications, such as a transmission protocol or a computer.

Auto Save — Zoning parameter that determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to permanent memory on that switch.

B

BootP Boot Strap Protocol. A type of network server.

Buffer Credit A measure of port buffer capacity equal to one frame.

C

Cascade Topology A fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology.

Class 2 Service A service which multiplexes frames at frame boundaries to or from one or more N_Ports wit h acknowledgment provided.

Chassis Hop A measure of fabric latency represented by the ISL that any frame crosses when travelling from one switch to another. A frame that travels from one switch to another over an ISL experiences one chassis hop.

Class 3 Service A service which multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment.

Configured Zone Sets The zone sets stored on a switch.

D

Device Security A component of fabric security that provides for the authorization and authentication of devices that attach to a switch through the use of groups and security sets.

Domain ID User defined number that identifies the switch in the fabric.

E

Element Manager See McDATA Element Manager.

Embedded Web Server See McDATA Embedded Web Server.

Event Log Log of messages describing events that occur in the fabric.

Expansion Port E_Port that connects to another FC-SW-2 compliant switch.

F

Fabric Database The set of fabrics that have been opened during a McDATA Embedded Web Server session.

Fabric Device Management Interface An interface by which device host bus adapters can be managed through the fabric.

Fabric Management Switch The switch through which the fabric is managed.

Fabric Name User defined name associated with the file that contains user list data for the fabric.

Fabric Port An F_Port or FL_Port.

Fabric Security The functions that provide security for fabric users and devices including user account security, and fabric services.

Fabric Services A component of fabric security that provides for the control of inband management and SNMP on a switch.

Fabric View File A file containing a set of fabrics that were opened and saved during a previous McDATA Embedded Web Server session.

FDMI See Fabric Device Management Interface.

Flash Memory Memory on the switch that contains the chassis control firmware.

Frame Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter.

FRU Field Replaceable Unit

G

Group A list of device worldwide names that are authorized to attach to a switch. There are three group types: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS).

I

Inband Management The ability to manage a switch through another switch over an inter-switch link.

Initiator The device that initiates a data exchange with a target device.

In-Order-Delivery A feature that requires that frames be received in the same order in which they were sent.

Input Power LED A chassis LED that indicates that the switch logic circuitry is receiving proper DC voltages.

Inter-Switch Link The connection between two switches using E_Ports.

IP Internet Protocol

L

LIP Loop Initialization Primitive sequence

Logged-In LED A port LED that indicates device login or loop initialization status.

M

Maintenance Button Momentary button on the switch used to reset the switch or place the switch in maintenance mode.

Maintenance Mode Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes.

Management Information Base A set of guidelines and definitions for SNMP functions.

Management Workstation PC workstation that manages the fabric through the fabric management switch.

McDATA Element Manager Switch management application that resides on the switch and is accessible through the EFCM.

McDATA Embedded Web Server Switch management application that resides on the switch an is accessible through an internet browser.

Mesh Topology A fabric in which each chassis has at least one port directly connected to each other chassis in the fabric.

MIB Management Information Base

Multistage Topology A fabric in which two or more edge switches connect to one or more core switches.

N

Network Time Protocol A network protocol that enables a client to synchronize its time with a server.

NL_Port Node Loop Port. A Fibre Channel device port that supports arbitrated loop protocol.

N_Port Node Port. A Fibre Channel device port in a point-to-point or fabric connection.

NTP Network Time Protocol

P

Pending Firmware The firmware image that will be activated upon the next switch reset.

POST Power-On Self Test

Power-On Self Test Diagnostics that the switch chassis performs at start up.

Principal Switch The switch in the fabric that manages domain ID assignments.

S

Simple Network Management Protocol An application protocol that manages and monitors network communications and functions. It also controls the Management Information Base (MIB).

Security Set A set of up to three groups with no more than one of each group type: ISL, Port, or MS. The active security set defines the device security for a switch.

SFP Small Form-Factor Pluggable.

Small Form-Factor Pluggable A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port.

SNMP Simple Network Management Protocol

Soft Zone Soft zoning divides the fabric for purposes of controlling discovery. Members of the same soft zone automatically discover and communicate freely with all other members of the same zone.

T

Target A storage device that responds to an initiator device.

U

User Account An object stored on a switch that consists of an account name, password, authority level, and expiration date.

User Account Security A component of fabric security that provides for the administration and authentication of account names, passwords, expiration dates, and authority level.

V

VCCI Voluntary Control Council for Interference

Voluntary Control Council for Interference A consortium of Japanese electronics industry associations that have established voluntary standards for controlling electromagnetic interference (EMI).

W

Worldwide Name (WWN) A unique 64-bit address assigned to a device by the device manufacturer.

WWN Worldwide Name

Z

Zone A set of ports or devices grouped together to control the exchange of information.

Zone Set A set of zones grouped together. The active zone set defines the zoning for a fabric.

Zoning Database The set of zone sets and zones stored on a switch.

Index

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Z

Notes